Network Address Translation (NAT)

The advantage of using private IP addresses is that it allows an organization to use private addressing in a network, and use the Internet at the same time, by implementing Network Address Translation (NAT). NAT is defined in RFC 1631 and allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet. Essentially, NAT allows hosts that use private addresses or addresses assigned to another organization, i.e. addresses that are not Internet-ready, to continue to be used and still allows communication with hosts across the Internet. NAT accomplishes this by using a valid registered IP address to represent the private address to the rest of the Internet. The NAT function changes the private IP addresses to publicly registered IP addresses inside each IP packet that is transmitted to a host on the Internet.

Variations of NAT

The Cisco IOS software supports several variations of NAT. These include Static NAT; Dynamic NAT; and Overloading NAT with Port Address Translation (PAT).

Static NAT

In Static NAT, the IP addresses are statically mapped to each other. Thus, the NAT router simply configures a one-to-one mapping between the private address and the registered address that is used on its behalf. Supporting two IP hosts in the private network requires a second static one-to-one mapping using a second IP address in the public address range, depending on the number of addresses supported by the registered IP address.

Dynamic NAT

Dynamic NAT is similar to static NAT in that the NAT router creates a one-to-one mapping between an inside local and inside global address and changes the IP addresses in packets as they exit and enter the inside network. However, the mapping of an inside local address to an inside global address happens dynamically. Dynamic NAT accomplishes this by setting up a pool of possible inside global addresses and defining criteria for the set of inside local IP addresses whose traffic should be translated with NAT.

With dynamic NAT, you can configure the NAT router with more IP addresses in the inside local address list than in the inside global address pool. When the number of registered public IP addresses is defined in the inside global address pool, the router allocates addresses from the pool until all are allocated. If a new packet arrives, and it needs a NAT entry, but all the pooled IP addresses are already allocated, the router discards the packet. The user must try again until a NAT entry times out, at which point the NAT function works for the next host that sends a packet. This can be overcome through the use of Port Address Translation (PAT).

Overloading NAT with Port Address Translation (PAT)

In some networks, most, if not all, IP hosts need to reach the Internet. If that network uses private IP addresses, the NAT router needs a very large set of registered IP addresses. If you use static NAT, each private IP host that needs Internet access needs a publicly registered IP address. Dynamic NAT lessens the problem, but if a large percentage of the IP hosts in the network need Internet access throughout normal business hours, a large number of registered IP addresses would also be required. These problems can be overcome through overloading with port address translation. Overloading allows NAT to scale to support many clients with only a few public IP addresses.

To support lots of inside local IP addresses with only a few inside global, publicly registered IP addresses, NAT overload uses Port Address Translation (PAT), translating the IP address as well as translating the port number. When NAT creates the dynamic mapping, it selects not only an inside global IP address but also a unique port number to use with that address. The NAT router keeps a NAT table entry for every unique combination of inside local IP address and port, with translation to the inside global address and a unique port number associated with the inside global address. And because the port number field has 16 bits, NAT overload can use more than 65,000 port numbers, allowing it to scale well without needing many registered IP addresses.

Translating Overlapping Addresses

NAT can also be used in organizations that do not use private addressing but use a network number registered to another company. If one organization uses a network number that is registered to another organization, and both organizations are connected to the Internet, NAT can be used to translate both the source and the destination IP addresses. However, both the source and the destination addresses must be changed as the packet passes through the NAT router.